REMARKS

The Office Action mailed December 12, 2005, has been received and reviewed. Claims 1-24 are currently pending in the application. Formerly numbered claim 13 has been objected to because of numbering informality. Claims 1-24 stand rejected. Applicant has amended claims 1, 11, 15, 22, 23, and 24, and respectfully request reconsideration of the application as amended herein.

I) Claim Objections

Claim 13 is objected to because of the following informalities: The claim appears to be number 3 rather than 13.

Applicant respectfully requests that the claim between claim 12 and claim 14 be properly numbered as claim 13 in accordance with the specific numbering given that claim in previous listings of the claims. Specifically, the second occurrence of misnumbered claim [3] has been renumbered as claim [13].

II) Claim Rejections

35 U.S.C. § 102(b) Anticipation Rejections

Anticipation Rejection Based on U.S. Patent No. 6,690,795 to Richards et al.

Claims 1-5, 10-11, 13-16 and 18-24 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Richards et al. (U.S. Patent No. 6,690,795). Applicant respectfully traverses this rejection, as hereinafter set forth.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Applicant submits that the Richards reference does not and cannot anticipate under 35 U.S.C. § 102 the presently claimed invention of claims 1-5, 10-11, 13-16 and 18-24 because the

Richards reference does not describe, either expressly or inherently, the identical inventions in as complete detail as are contained in the claims.

The Office Action alleges:

> Regarding claims 1-5, 11, 13-14 & 22-24, Richards discloses determining a registration key/UEV specific to a participant/set top box in a transmission (Fig. 26, #130), determining a first key/CCK_1 (Fig. 26, #133), encrypting the first key/CCK_1 with the registration key (Fig. 26, #133), ***determining a second key/PK and SK***, encrypting the second key with the first key ([PK]CCK_1, [SK]PK) updating the first key/CCK after a first time period has elapsed (Fig. 23) and updating the second key/SK and PK after a second time period has elapsed, ***wherein the second key is updated in two parts (SK and PK), the first part/PK known to the participant in the transaction and a second part/SK sen[t] on a broadcast channel***(Fig. 26). (Office Action, p. 3; emphasis added.)

Claims 1-5, 10

Applicant respectfully disagrees that the Richards reference anticipates Applicant's invention as claimed in presently amended independent claim 1 which reads:

> 1. A method for secure transmissions, the method comprising:
> determining a registration key specific to a participant in a transmission;
> determining a first key;
> encrypting the first key with the registration key;
> sending the encrypted first key to the participant in the transmission;
> ***determining a second key for decrypting content on a broadcast channel;***
> encrypting the second key with the first key;
> ***updating the first key after a first time period has elapsed; and***
> ***updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***
> (Emphasis added.)

In contrast, the Richards reference discloses:

> CCK_1 is delivered ... as [CCK_1]UEV, wherein UEV is the customer's User Encryption Variable .... (Richards, col. 15, lines 8-10).
> When decrypted in block 133, CCK_1 is obtained, which is fed to block 138, on line 135. Block 138 uses the data [CCK_1] on line 135 as the key to decrypt its input from the in-band channel 6. (Richards, col. 15, lines 11-14).

Thus, if the UEV of the Richards reference is equated to Applicant's claimed element of a "registration key" then the CCK_1 of the Richards reference would equate to Applicant's claimed element of a "first key."

The Richards reference continues to disclose:

> Thus, block 138 uses CCK_1 as a key to decrypt [*CCK_1*]CCK_1, as indicated within the block, to produce *CCK_1* on line 140 .... (Richards, col. 15, lines 16-18; emphasis added).

The "first key" or unbold and unitalicized CCK_1 is used to decrypt the bold and italicized ***CCK_1*** (e.g., a subsequent or "second Richards key") which is the key used to decrypt [PK]***CCK_1*** in block 144 of FIG. 26. As evidenced in FIG. 26 of the Richards reference, PK (e.g., a yet subsequent or "third Richards key") is further used to decrypt [SK]PK in block 152 of FIG. 26. As further evidenced in FIG. 26 of the Richards reference, SK (e.g., a further subsequent or ***"fourth Richards key") is used to decrypt [CONTENT]SK*** in block 159 of FIG. 26, as opposed to Applicant's claimed element of "***a second key for decrypting content*** on a broadcast channel".

Clearly the Richards reference discloses decrypting content using a key, however, the Richards reference discloses decrypting content with SK which is at least a "fourth Richards key". Nothing in the Richards reference discloses Applicant's claimed element of the invention of "***determining a second key for decrypting content on a broadcast channel***".

Furthermore, Applicant's invention as presently claimed with respect to amended independent claim 1 recites, "updating the first key after a first time period has elapsed; and ***updating the second key after a second time period has elapsed***, wherein ***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***" The Richards reference does not disclose updating the "second Richards key", namely *CCK_1* and the Richards reference is certainly silent regarding Applicant's claimed element of the invention of "***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel***" As is clear from FIG. 26 of the Richards reference, both the PK and SK parts, as alleged in the Office Action, arrive from the in-band channel 6 and, therefore, neither part can be "known to the participant" as presently claimed in Applicant's amended independent claim 1.

Therefore, the Richards reference cannot anticipate under 35 U.S.C. §102 Applicant's invention as presently claimed in amended independent claim 1. Accordingly, Applicant respectfully requests the rejection of claim 1, and claims 2-5 and 10 depending therefrom, be withdrawn as such claims are allowable over the cited reference.

Claims 11, 13, 14

Applicant respectfully disagrees that the Richards reference anticipates Applicant's invention as claimed in presently amended independent claim 11 which reads:

> 11. A method for secure reception of a transmission, the method comprising:
> receiving a registration key specific to a participant in a transmission;
> receiving a first key encrypted with the registration key;
> decrypting the first key with the registration key;
> ***receiving a second key for decrypting content on a broadcast channel;***
> ***decrypting the second key with the first key;***
> receiving a broadcast stream of information; and
> decrypting the broadcast stream of information using the second key;
> ***receiving an updated first key after a first time period has elapsed; and***
> ***receiving an updated second key after a second time period has elapsed,***
> ***wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.*** (Emphasis added.)

Applicant herein sustains the above-proffered arguments relating to the disclosure of the Richards reference. Clearly the Richards reference discloses decrypting content using a key, however, the Richards reference discloses decrypting content with SK which is at least a "fourth Richards key". Nothing in the Richards reference discloses Applicant's claimed element of the invention of "***receiving a second key for decrypting content on a broadcast channel; decrypting the second key with the first key***".

Furthermore, Applicant's invention as presently claimed with respect to amended independent claim 11 recites, "***receiving an updated first key after a first time period has elapsed; and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***"

The Richards reference does not disclose updating the "second Richards key", namely ***CCK_1*** and the Richards reference is certainly silent regarding Applicant's claimed element of the invention of "***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***" As is clear from FIG. 26 of the Richards reference, both the PK and SK parts, as alleged in the Office Action, arrive from the

in-band channel 6 and, therefore, neither part can be "known to the participant" as presently claimed in Applicant's amended independent claim 11.

Therefore, the Richards reference cannot anticipate under 35 U.S.C. §102 Applicant's invention as presently claimed in amended independent claim 11. Accordingly, Applicant respectfully requests the rejection of claim 11, and claims 13 and 14 depending therefrom, be withdrawn as such claims are allowable over the cited reference.

Claims 15, 16, 18-21

Applicant respectfully disagrees that the Richards reference anticipates Applicant's invention as claimed in presently amended independent claim 15 which reads:

> 15. In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:
>
> a receive circuitry adapted to receive a registration key specific to a participant in a transmission, receive a first key encrypted with the registration key, ***receiving a second key for decrypting content on a broadcast channel encrypted with the first key, receiving an updated first key after a first time period has elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel***;
>
> a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:
>
> processing unit operative to decrypt key information;
>
> memory storage unit for storing a registration key; and
>
> a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message. (Emphasis added.)

Applicant herein sustains the above-proffered arguments relating to the disclosure of the Richards reference. Clearly the Richards reference discloses decrypting content using a key, however, the Richards reference discloses decrypting content with SK which is at least a "fourth Richards key". Nothing in the Richards reference discloses Applicant's claimed element of the invention of "***receiving a second key for decrypting content on a broadcast channel encrypted with the first key***".

Furthermore, Applicant's invention as presently claimed with respect to amended independent claim 15 recites, "***receiving a second key for decrypting content on a broadcast channel encrypted with the first key, receiving an updated first key after a first time period has***

elapsed, and receiving an updated second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel".

The Richards reference does not disclose updating the "second Richards key", namely *CCK_I* and the Richards reference is certainly silent regarding Applicant's claimed element of the invention of "***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***" As is clear from FIG. 26 of the Richards reference, both the PK and SK parts, as alleged in the Office Action, arrive from the in-band channel 6 and, therefore, neither part can be "known to the participant" as presently claimed in Applicant's amended independent claim 15.

Therefore, the Richards reference cannot anticipate under 35 U.S.C. §102 Applicant's invention as presently claimed in amended independent claim 15. Accordingly, Applicant respectfully requests the rejection of claim 15, and claims 16, 18-21 depending therefrom, be withdrawn as such claims are allowable over the cited reference.

Claim 22

Applicant respectfully disagrees that the Richards reference anticipates Applicant's invention as claimed in presently amended independent claim 22 which reads:

> 22. A wireless communication system, comprising:
> means for determining a registration key specific to a participant in a transmission;
> means for determining a first key;
> means for encrypting the first key with the registration key;
> means for sending the encrypted first key to the participant in the transmission;
> ***means for determining a second key for decrypting content on a broadcast channel***;
> means for encrypting the second key with the first key;
> ***means for updating the first key after a first time period has elapsed; and***
> ***means for updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.*** (Emphasis added.)

Applicant herein sustains the above-proffered arguments relating to the disclosure of the Richards reference. Clearly the Richards reference discloses decrypting content using a key, however, the Richards reference discloses decrypting content with SK which is at least a "fourth

Richards key". Nothing in the Richards reference discloses Applicant's claimed element of the invention of "***means for determining a second key for decrypting content on a broadcast channel***".

Furthermore, Applicant's invention as presently claimed with respect to amended independent claim 22 recites, "means for updating the first key after a first time period has elapsed; and means for ***updating the second key after a second time period has elapsed***, wherein ***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***"

The Richards reference does not disclose updating the "second Richards key", namely *CCK_1* and the Richards reference is certainly silent regarding Applicant's claimed element of the invention of "***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***" As is clear from FIG. 26 of the Richards reference, both the PK and SK parts, as alleged in the Office Action, arrive from the in-band channel 6 and, therefore, neither part can be "known to the participant" as presently claimed in Applicant's amended independent claim 22.

Therefore, the Richards reference cannot anticipate under 35 U.S.C. §102 Applicant's invention as presently claimed in amended independent claim 22. Accordingly, Applicant respectfully requests the rejection of claim 22 be withdrawn as such claim is allowable over the cited reference.

Claim 23

Applicant respectfully disagrees that the Richards reference anticipates Applicant's invention as claimed in presently amended independent claim 23 which reads:

> 23. An infrastructure element, comprising:
> means for receiving a registration key specific to a participant in a transmission;
> means for receiving a first key encrypted with the registration key;
> means for decrypting the first key with the registration key;
> ***means for receiving a second key for decrypting content on a broadcast channel;***
> ***means for decrypting the second key with the first key;***
> means for receiving a broadcast stream of information; and
> means for decrypting the broadcast stream of information using the second key;
> ***means for updating the first key after a first time period has elapsed; and***
> ***means for updating the second key after a second time period has elapsed,***
> ***wherein the second key is updated in two parts, a first part known to the***

participant in the transmission and a second part sent on the broadcast channel. (Emphasis added.)

Applicant herein sustains the above-proffered arguments relating to the disclosure of the Richards reference. Clearly the Richards reference discloses decrypting content using a key, however, the Richards reference discloses decrypting content with SK which is at least a "fourth Richards key". Nothing in the Richards reference discloses Applicant's claimed element of the invention of "***means for receiving a second key for decrypting content on a broadcast channel; means for decrypting the second key with the first key***".

Furthermore, Applicant's invention as presently claimed with respect to amended independent claim 23 recites, "***means for updating the first key after a first time period has elapsed; and means for updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***"

The Richards reference does not disclose updating the "second Richards key", namely *CCK_1* and the Richards reference is certainly silent regarding Applicant's claimed element of the invention of "***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***" As is clear from FIG. 26 of the Richards reference, both the PK and SK parts, as alleged in the Office Action, arrive from the in-band channel 6 and, therefore, neither part can be "known to the participant" as presently claimed in Applicant's amended independent claim 23.

Therefore, the Richards reference cannot anticipate under 35 U.S.C. §102 Applicant's invention as presently claimed in amended independent claim 23. Accordingly, Applicant respectfully requests the rejection of claim 23 be withdrawn as such claim is allowable over the cited reference.

Claim 24

Applicant respectfully disagrees that the Richards reference anticipates Applicant's invention as claimed in presently amended independent claim 24 which reads:

24. A digital storage device, comprising:

first set of instructions for receiving a registration key specific to a participant in a transmission;
second set of instructions for receiving a first key encrypted with the registration key;
third set of instructions for decrypting the first key with the registration key;
fourth set of instructions for receiving a second key for decrypting content on a broadcast channel;
fifth set of instructions for decrypting the second key with the first key;
sixth set of instructions for receiving the broadcast stream of information; and
seventh set of instructions for decrypting the broadcast stream of information using the second key;
eighth set of instructions for updating the first key after a first time period has elapsed, updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel. (Emphasis added.)

Applicant herein sustains the above-proffered arguments relating to the disclosure of the Richards reference. Clearly the Richards reference discloses decrypting content using a key, however, the Richards reference discloses decrypting content with SK which is at least a "fourth Richards key". Nothing in the Richards reference discloses Applicant's claimed element of the invention of "***fourth set of instructions for receiving a second key for decrypting content on a broadcast channel***".

Furthermore, Applicant's invention as presently claimed with respect to amended independent claim 24 recites, "***eighth set of instructions for updating the first key after a first time period has elapsed, updating the second key after a second time period has elapsed, wherein the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on a broadcast channel.***"

The Richards reference does not disclose updating the "second Richards key", namely *CCK_1* and the Richards reference is certainly silent regarding Applicant's claimed element of the invention of "***the second key is updated in two parts, a first part known to the participant in the transmission and a second part sent on the broadcast channel.***" As is clear from FIG. 26 of the Richards reference, both the PK and SK parts, as alleged in the Office Action, arrive from the in-band channel 6 and, therefore, neither part can be "known to the participant" as presently claimed in Applicant's amended independent claim 24.

Therefore, the Richards reference cannot anticipate under 35 U.S.C. §102 Applicant's invention as presently claimed in amended independent claim 24. Accordingly, Applicant respectfully requests the rejection of claim 24 be withdrawn as such claim is allowable over the cited reference.

35 U.S.C. § 103(a) Obviousness Rejections

Obviousness Rejection Based on U.S. Patent No. 6,690,795 to Richards et al. in view of FOLDOC

Claim 6 was rejected as being unpatentable over U.S. Patent 6,690,795 to Richards as applied to claim 4 in further view of "FOLDOC, Free On-Line Dictionary of Computing" by LinuxGuruz (hereinafter "FOLDOC"). Applicant respectfully traverses this rejection, as hereinafter set forth.

The nonobviousness of presently amended independent claim 1 precludes a rejection of claim 6 which depends therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Applicant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 6 which depends from presently amended independent claim1.

Obviousness Rejection Based on U.S. Patent No. 6,690,795 to Richards et al. in view of Schneier

Claims 7-9 were rejected as being unpatentable over U.S. Patent 6,690,795 to Richards as applied to claim 3 in further view of Applied Crytography, Second Edition by Schneier. This rejection is respectfully traversed.

The nonobviousness of presently amended independent claim 1 precludes a rejection of claims 7-9 which depend therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Applicant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 7-9 which depend from presently amended independent claim1.

Obviousness Rejection Based on U.S. Patent No. 6,690,795 to Richards et al. in view of U.S. Patent No. 6,073,122 to Wool

Claim 12 and 17 was rejected as being unpatentable over U.S. Patent 6,690,795 to Richards as applied to claim 11 and 15 in further view of U.S. Patent 6,073,122 to Wool (hereinafter "Wool"). This rejection is respectfully traversed.

The nonobviousness of presently amended independent claims 11 and 15 preclude a rejection of claims 12 and 17 which respectively depend therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Applicant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejections to claims 12 and 17 which respectively depend from presently amended independent claims 11 and 15.

PATENT

CONCLUSION

Claims 1-24 are believed to be in condition for allowance, and an early notice thereof is respectfully solicited. Should the Examiner determine that additional issues remain which might be resolved by a telephone conference, the Examiner is respectfully invited to contact Applicant's undersigned attorney.

Respectfully submitted,

Dated: June 8, 2006

By: Ramin Mobarhan
Ramin Mobarhan, Reg. No. 50,182
Phone: (858) 658-2447

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-2447
Facsimile: (858) 658-2502